MicroStrategy Cloud Enterprise – User Guide Version 1.1

SERVICE DEFINITION AND POLICIES

FEBRUARY 21, 20132/21/2013

TABLE OF CONTENTS

MICROSTRATEGY CLOUD PLATFORM OVERVIEW

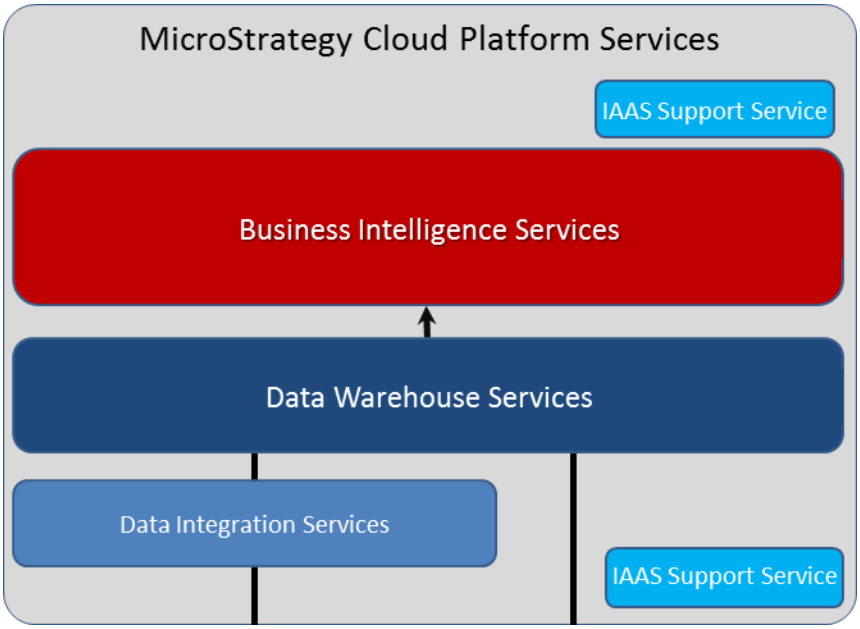
OVERVIEW OF OPERATIONS

MicroStrategy is a global provider of enterprise software platforms for business intelligence (BI), mobile intelligence, and social intelligence applications. MicroStrategy provides integrated reporting, analysis, and monitoring software that enables companies to analyze the data stored across their enterprise or in the Cloud to make better business decisions. MicroStrategy Cloud is a division of MicroStrategy responsible for delivering MicroStrategy cloud based services. MicroStrategy Cloud offers both a Platform as a Service (PAAS) known as MicroStrategy Cloud Platform, and Software as a Service (SAAS) models known as MicroStrategy Cloud Personal and MicroStrategy Cloud Express and a small scale Infrastructure offering to support business intelligence applications in the cloud.

WHAT IS MICROSTRATEGY CLOUD PLATFORM?

MicroStrategy Cloud Platform delivers a complete business analytics platform-as-a-service, including business intelligence, data integration and data warehouse capabilities. . MicroStrategy Cloud Platform is a public cloud service that offers the following services:

- MicroStrategy's business intelligence platform for both mobile and web;
- Data hosting capabilities on a variety of database management systems. Data hosting is used primarily for the purposes of building a data warehouse or data marts, but can be extended to include a variety of other database needs.
- Data integration services which allows for extraction, transformation and loading data into data sources in the MicroStrategy Cloud environment
- Infrastructure Services to allow customers to install, manage, and run business intelligence related applications not natively hosted within the MicroStrategy Cloud Platform.



MicroStrategy Cloud Services are designed to transform and simplify the manner in which analytics solutions are built and delivered within an organization. They are designed to provide customers an environment to host, transform, analyze, and report data through the MicroStrategy Business Intelligence framework and cloud hosting services. The services offering provides a menu of data warehouse, data integration, and reporting capabilities. As subscribers to the MicroStrategy Cloud Platform customers are required to use the Business Intelligence Services, but the other Platform Services are available as options.

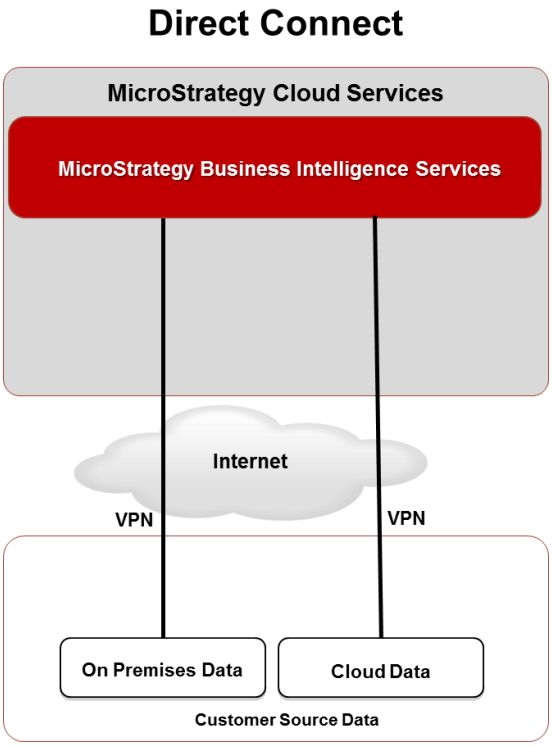
The MicroStrategy Cloud is centered on the MicroStrategy Business Intelligence Services. It provides customers' access to the MicroStrategy Business Intelligence products as a hosted cloud service. Customers can select from a list of product options which are hosted on a shared infrastructure.

MicroStrategy Cloud Data Warehouse Services (MCDW) provides access to relational database capabilities. A tiered set of services are available from small transactional databases to complex enterprise data warehousing environments.

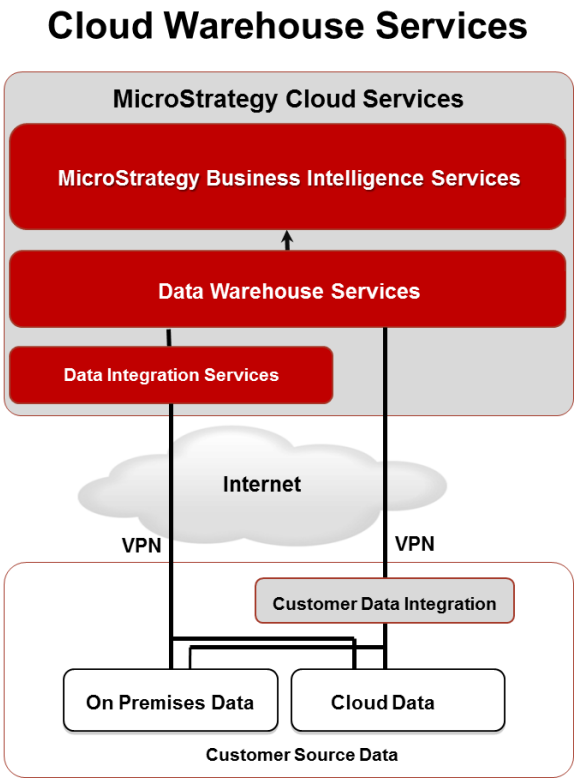
The MicroStrategy Cloud Data Integration Service (MCDIS) is designed to move data into the MicroStrategy Cloud Data Warehouse environment. The service provides capabilities that support data acquisition from varied multiple data sources including; data extraction, validation, transformation and loading.

PRIMARY CONFIGURATION OPTIONS

There are two primary configuration options with MicroStrategy Cloud. The first is a BI-only, "Direct Connect" service. In this case, the primary data warehouse or data mart(s) reside on-premise (or in another public or private cloud). The MicroStrategy Cloud BI layer operates directly against the on-premise database(s). Data integration capabilities in this scenario are also maintained by the customer alongside the data warehouse. Such a configuration is ideally suited to companies that have made recent investments in database or data integration platforms.



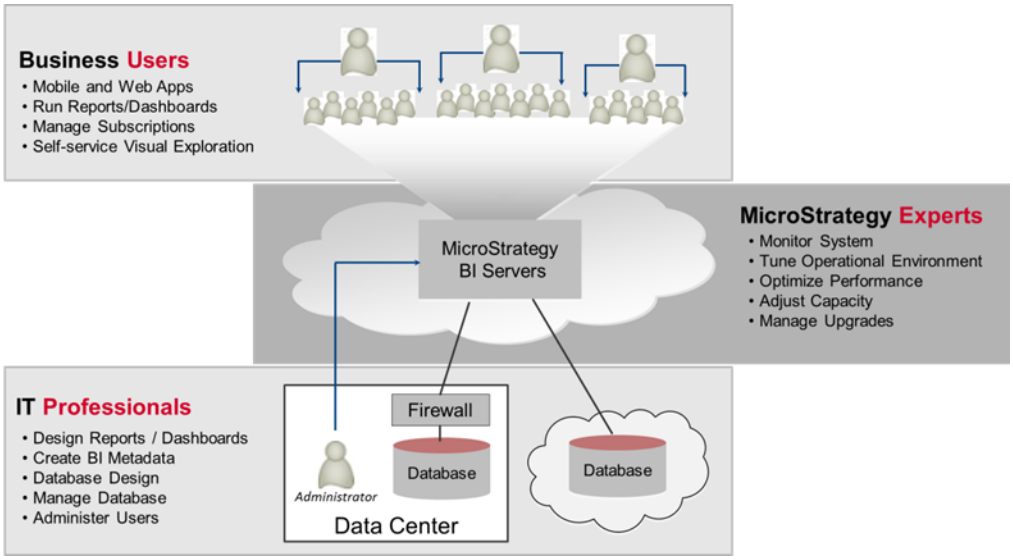
The second is a BI with data services configuration. With this setup, the primary data warehouse and data integration software, resides within the MicroStrategy Cloud along with the BI server itself. This configuration has the added benefit of having components of the analytics platform in a single infrastructure. The MicroStrategy Cloud service level agreement will correspondingly apply to this entire stack.



While these are the two primary configurations, customers often have specific requirements which do not conform precisely to either setup. These configurations are not exclusive with MicroStrategy multi-source a standard component of the MicroStrategy Cloud BI Service. This enables connecting Direct Connect and Cloud Warehouse Services to the same customer environment. In these cases, MicroStrategy Cloud offers the flexibility to customize the configuration to meet virtually any requirement.

CLOUD SERVICE RESPONSIBILITIES

The MicroStrategy Cloud Platform Services are designed to make it quicker, easier, and more cost effective for our customers to implement business intelligence solutions. With MicroStrategy Cloud Platform Services, business users are able to take advantage of the MicroStrategy Business Intelligence Services to analyze their data, IT Professionals are able to focus on building out valuable business intelligence solutions, and the MicroStrategy Cloud Team is focused on managing, monitoring, optimizing, and running the MicroStrategy Cloud Platform Services.



To support our offering, MicroStrategy has deployed a dedicated organization focused on supporting the MicroStrategy cloud environment. This organization includes managing environment setup, configuration, monitoring, as well as additional responsibilities designed to provide high availability and performance of the environment. MicroStrategy is responsible for managing the physical implementation of the MicroStrategy Cloud Platform infrastructure and restricts customer access to the server instances running the MicroStrategy Cloud, outside of the Infrastructure as a Service offering. As part of Cloud Platform services, MicroStrategy manages patching the environments at the server and application level, excluding IaaS customer installed applications.

Customers are responsible for the configuration, development, change management, administration, and support of the business intelligence application, data warehouse, and data integration transformations. In addition, application performance tuning and optimizations are the responsibility of the customer. If desired, MicroStrategy Professional Services can be contracted to provide or assist with system tuning. Data loading, data quality, and cleansing also are responsibilities of the customers. MicroStrategy offers various Data Integration service options that can be leveraged to load and validate data in the customer environment.

MICROSTRATEGY CLOUD BUSINESS INTELLIGENCE SERVICES

MICROSTRATEGY BUSINESS INTELLIGENCE PLATFORM FEATURES

At the core of the MicroStrategy Cloud is the MicroStrategy Business Intelligence Services. The Business Intelligence Services provide customers' access to the MicroStrategy Business Intelligence product catalog hosted as a cloud service. Customers can select from a list of product options which are hosted on a shared infrastructure. Customer environments are configured in a single-tenant virtualized environment pre-configured and optimized for use at start-up. As a result of pre-configuring the various products, customers can take advantage of the MicroStrategy capabilities immediately when starting with the MicroStrategy Cloud Business Intelligence Service, with additional capabilities enabled at the customer request.

MicroStrategy has engineered its platform to help deliver an integrated architecture that scales to support enterprise level business intelligence. This enterprise scale integrated architecture is well suited for the Cloud, and the MicroStrategy Cloud ™ service offering takes advantage of the platform to build, scale, and manage the Cloud service. Management services like clustering, security, user management, and resource management help provide a highly available environment that can scale up or out to meet the most demanding business intelligence requirements.

MicroStrategy platform features that are part of the standard cloud offering, as well as optional choices and a Professional Services offering, are shown in the table below:

MICROSTRATEGY CAPABILITIES FOR CLOUD SERVICES

	Cloud User Types					
MicroStrategy Product	Mobile User	Consumer User	Analyst User	Power User	Desktop Designer	Architect
Intelligence Server w/ Clustering	√	√	√	√	√	√
Distribution Services	*	√	√	√	√	√
Multi-source	√	√	√	√	√	√
OLAP Services	√	√	√	√	√	√
Report Services	√	√	√	√	√	√
Iserver Universal	√	√	√	√	√	√
Web Reporter	⊘	√	√	√	√	√
Web Universal	⊘	√	√	√	√	√
Mobile	√	O	O	O	√	√
Office	⊘	⊘	√	√	√	√
Transaction Services	O	O	O	O	√	√
Web Analyst	⊘	⊘	√	√	√	√
Web Professional	⊘	⊘	⊘	√	√	√
Desktop Designer**	⊘	⊘	⊘	⊘	√	√
Architect	⊘	⊘	⊘	⊘	⊘	√
MicroStrategy SDK – look and feel or security customization	⊘	⊘	⊘	⊘	⊘	√
MicroStrategy SDK – other customizations	⊘	⊘	⊘	⊘	⊘	O

* Mobile-Only licenses may receive Mobile-only push subscriptions only.

**MicroStrategy Desktop is a development only tool in the MicroStrategy Cloud used by architects and report developers to deliver reports via web, mobile, office, or distribution services. The tool is hosted via WebVPN in a virtual desktop.

SUPPORTED MICROSTRATEGY CLOUD VERSIONS

MicroStrategy Cloud keeps customers on current stable versions of the MicroStrategy platform. Currently supported versions of MicroStrategy in the cloud include:

- MicroStrategy 9.2.1m
- MicroStrategy 9.3

BUSINESS INTELLIGENCE SERVICES AND CUSTOMER RESPONSIBILITY

Cloud Business Intelligence customers are responsible for developing their own custom business intelligence and mobile applications using the Business Intelligence Services. This development can be performed through their own internal development resources, third party consulting services, or MicroStrategy Professional Services. While customers are able to focus on developing solutions that provide business value, the MicroStrategy Cloud service provides the monitoring, management, and optimization of the Business Intelligence environment. Customers are able to configure various components of their cloud environment or work with the MicroStrategy Cloud team to set configuration values.

The table below breaks down major categories of services and activities related to management of a MicroStrategy Cloud Platform environment. Premium services are available for an additional charge. Optional managed services are delivered by MicroStrategy's Professional Services organization and are not part of the standard MicroStrategy Cloud Platform offering.

Service	Cloud Platform Team Support	Customer Responsibility	Optional – Managed Services*
Administration			
Managing MicroStrategy Groups and Users		✓	✓
Controlling access to application functionality	✓	O	
Controlling access to data		✓	✓
Monitoring user access	✓	✓	
Maintaining caches	✓	✓	
Maintaining Intelligent Cubes	✓	✓	
Maintaining History Lists	✓		
Scheduled administrative services	✓		
Maintaining report schedules and subscriptions		✓	✓
Administering report delivery (Distribution Services)		✓	✓
Administering report delivery (Narrowcast Services)		✓	✓
Advanced application performance tuning – reports, caches, cubes, etc.			✓
Performance Tesing and Monitoring			
Up front customized Cloud performance assessment			✓
Monitoring system usage	✓	✓	
Analyzing system usage and application performance		✓	✓
MicroStrategy Architect Metadata Development			
Creating logical business model / metadata objects		✓	✓
MicroStrategy Report and Dashboard Development			
Creating reports		✓	✓
Designing dashboards		✓	✓
Defining metrics		✓	✓
Defining filters		✓	✓
Creating templates		✓	✓
Change Management and Change Control			
Managing MicroStrategy objects		✓	✓
MicroStrategy Project and Object Migration	✓	✓	
Platform planning and execution	✓		

DATA INTEGRATION

The MicroStrategy Cloud Data Integration Service (MCDIS) is an optional service that enables customers to move data into the MicroStrategy Cloud Data Warehouse environment. The service provides a wide array of options to support data acquisition from varied data sources, data movement, data transformation, and data loading. The service is configured to work with MicroStrategy Cloud Data Warehouse Service (MCDW), with the Data Integration service tied to only loading data into the MicroStrategy Cloud Data Warehouse Services.

The service options can be selected based on the features required to extract, transform, validate, and load data. Options can be included depending on the type of connectivity between you and the MCDWS environment. The MicroStrategy Cloud team will assist in reviewing the options to help determine the tiers of service that would be required to support customer needs.

Customers that opt to maintain their data integration solutions on-premises can use these solutions alongside MicroStrategy Cloud, as long as proper connectivity between the customer network and MicroStrategy can be established.

MICROSTRATEGY CLOUD AND CUSTOMER RESPONSIBILITY

MicroStrategy provides management, monitoring, and physical environment administrative functionality for the data integration capabilities. The administration offerings include environment setup, configuration, monitoring, as well as additional services designed to maintain high availability of the data integration environment. MicroStrategy is responsible for managing the physical implementation of the Data Integration Services and restricts access to the server instances running the data integration services. As part of the warehouse services, MicroStrategy manages patching the environments at the server and database level.

MicroStrategy customers are responsible for logical administration and development of data integration transformations, tasks, and jobs in the MicroStrategy Cloud including development of ETL transformation, data profiling, data quality and validation, managing schedules, and monitoring of ETL process execution. In addition, ETL performance tuning and optimizations are the responsibility of the customer. MicroStrategy customers are also responsible for implementing security as part of the ETL process. If encryption or additional data security is required as part of the transformation process, the customer is responsible for implementing security practices as part of their design and implementation. MicroStrategy personnel will have limited access to customer environments and data with only critical administrators and support person specifically granted access by the customer. As a result, customers are responsible for all data they place in the MicroStrategy Cloud Data Warehouse service.

TOOLS PARTNER

MicroStrategy has partnered with Informatica to deliver data integration tools that support both ease of use and full-featured transformations. The services available include Informatica's Power Center platform and cloud capabilities. These capabilities can be used separately or be combined to support various data integration requirements.

Some of the Data Integrations services provided in the MicroStrategy Cloud, specifically the Informatica Cloud, are provided by Informatica. As a result, our partner Informatica will be responsible for the management, monitoring, and maintenance of the Informatica Cloud metadata services. MicroStrategy will have responsibility for the Informatica Cloud agent services which are maintained within the MicroStrategy Cloud customer environment.

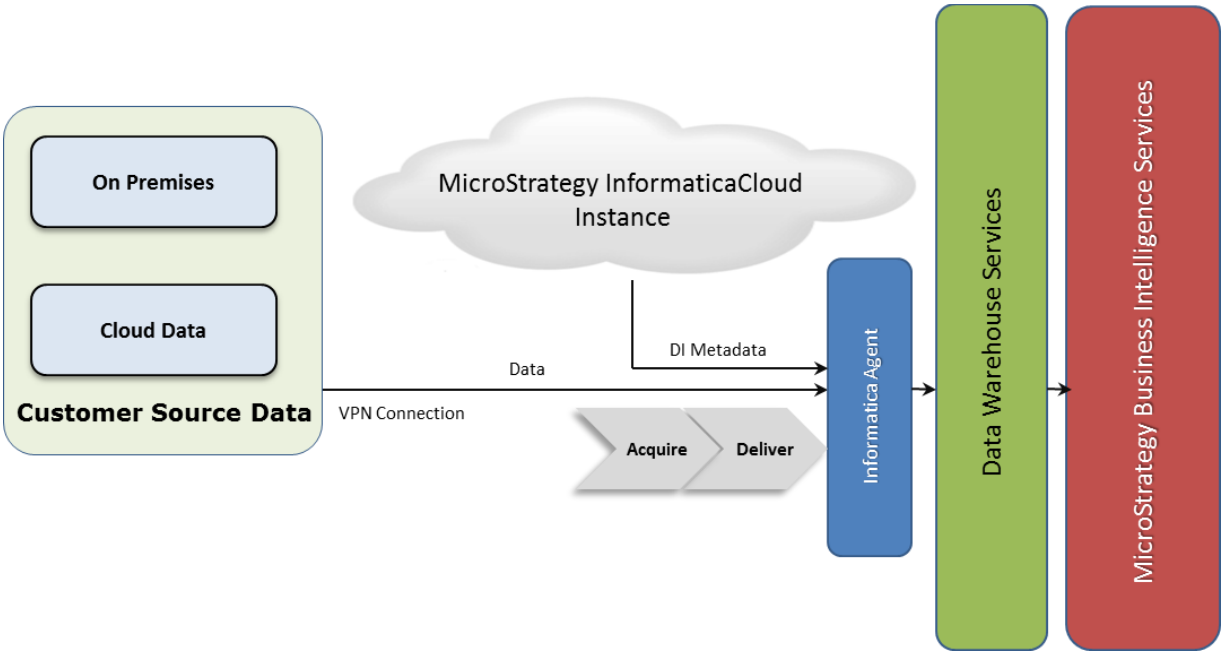
The MicroStrategy Cloud Data Integration capability based on Informatica Power Center capabilities are hosted and managed by the MicroStrategy Cloud team. These services are managed, monitored, and maintained by the MicroStrategy Technical Operations team.

SERVICE OPTIONS

MCDIS provides multiple options to support customer requirements. The service options can be selected based on the features required to extract, transform, validate, and load data. Options can be combined depending on your type of connectivity with the MCDWS environment. The MicroStrategy Cloud Platform team can help determine the tiers of service required for your needs.

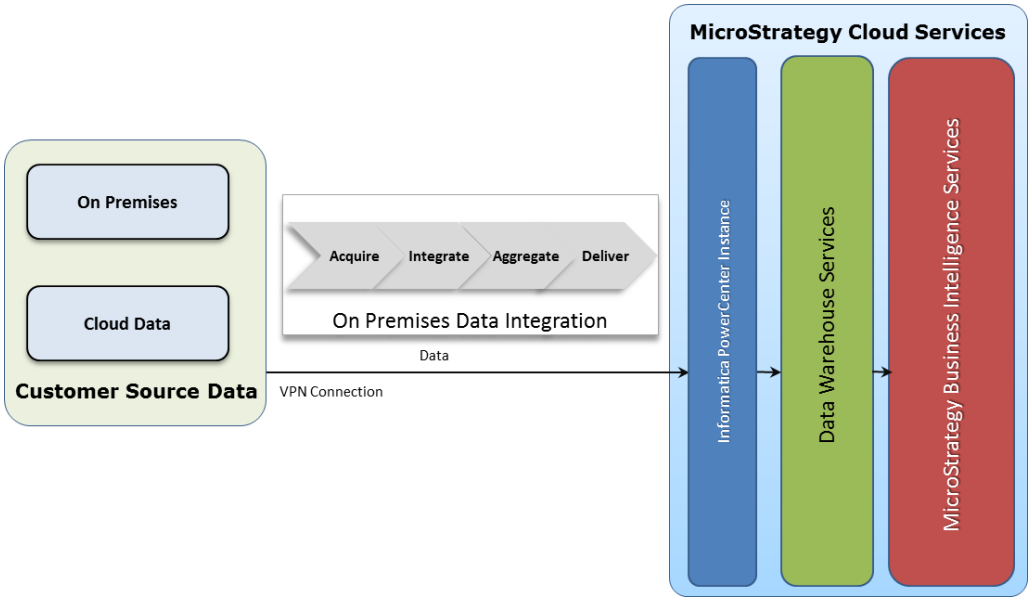
CLOUD SERVICES OPTION

The Cloud Services Option is ideal for situations when you are moving from an on-premises data source or third-party cloud data source, and the data warehouse requires simple transformations or direct replication of data structures between the source and destination databases. This solution requires that connectivity be established between the customer data source and the MicroStrategy Cloud.



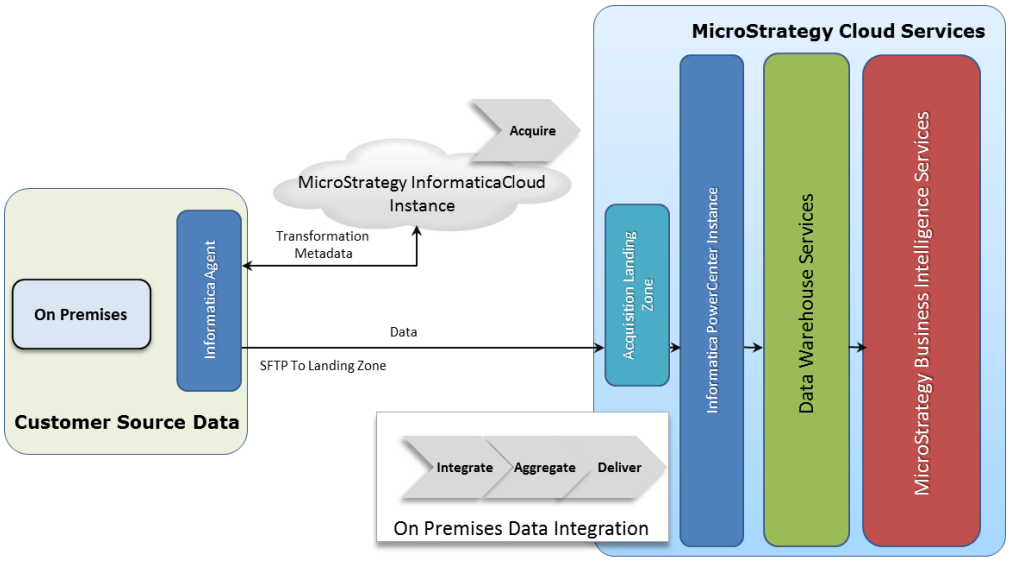
DATA INTEGRATION IN MICROSTRATEGY CLOUD

Data integration in MicroStrategy Cloud uses an instance of Informatica Power Center to manage transformations. This instance can be dedicated to a customer or can be set up as part of a shared instance. This solution also requires that connectivity be established directly from the customer site to the MicroStrategy Cloud environment.



CLOUD AND ON-PREMISES

If it is not possible to establish a secure connection between your network and MicroStrategy, it may be possible to move data to files and then load data from those files into the MicroStrategy Data Warehouse. In this case, the Informatica Cloud agent is installed at your site. The agent can be used to pull data from your data sources and push the results via secure FTP to a secure data store in the MicroStrategy Cloud. From that location, either the Informatica Cloud services or Informatica Power Center can be used to load data into your data warehouse instances.



MICROSTRATEGY CLOUD DATA WAREHOUSE SERVICES

SERVICE OPTIONS

MicroStrategy Cloud Data Warehouse Services provides a tiered set of relational database capabilities designed for data warehousing and configured to support customer data analysis requirements. The MicroStrategy Cloud team offers the tiers of service required by a customer based on a number of factors. These factors include database size, database growth projections, performance requirements, disaster recovery and SLA, security, encryption, and other dynamics. Analysis to determine the appropriate tier of service is typically performed during the analysis phase of the customer engagement. Customer input will be taken into account when selecting tiers and database vendors, but MicroStrategy reserves the right to determine the data warehouse platform for customer applications. The following tiers of service are available:

- **Basic Edition**. The basic edition is the most cost effective option, designed for small scale data warehouse solutions. This solution is designed to support a maximum data volume of 1 TB. This option features a low compute-to-storage ratio, a low memory-to-storage ratio, and standard disks.
- **Performance Edition**. Based on a standard data warehouse appliance offering from a leading analytical database vendor, this option delivers strong performance and scalability. This option features a medium compute-to-storage ratio, a medium memory-to-storage ratio, and fast disks.
- **Enterprise Edition**. Based on a high end appliance from a leading analytical database vendor, this option is designed to support use cases with large amounts of data, high levels of concurrency and demanding analytical challenges. This option features a high compute-to-storage ratio, a high memory-to-storage ratio, and very high performance disks.

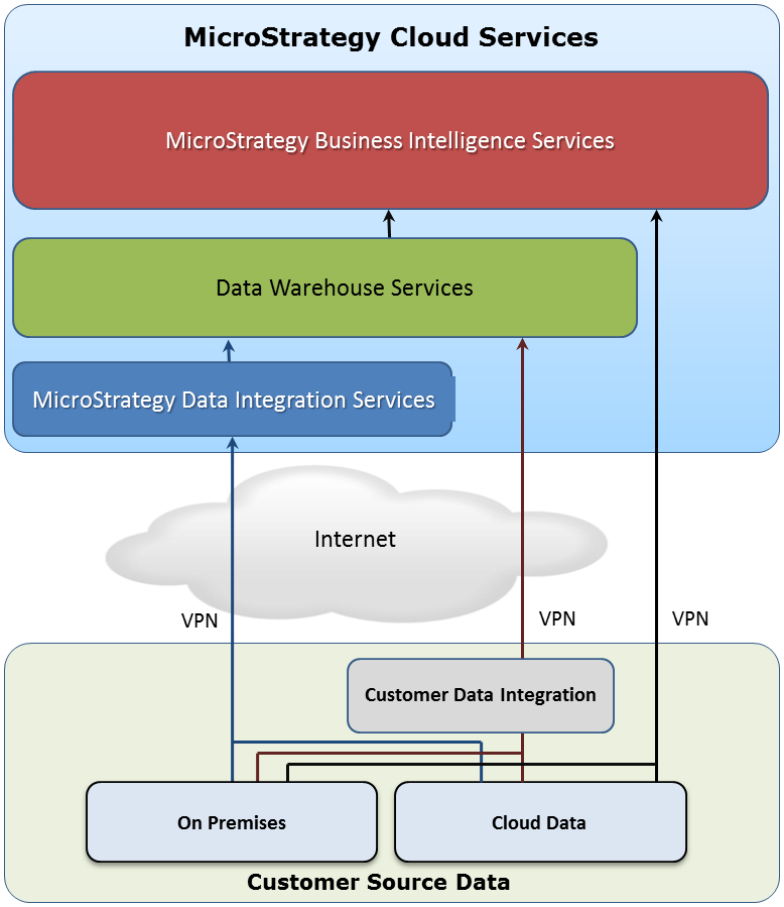
MicroStrategy partners with several vendors to provide performance and platform editions of the MCDWS. These vendors provide level-3 support for MicroStrategy Cloud. Should a customer's data warehouse need to move to another performance tier, MicroStrategy Cloud operations managers and MicroStrategy Professional Services work with the customer to plan and execute the operation.

WAREHOUSE CONNECTIVITY

MicroStrategy Cloud Business Intelligence Services can connect to databases or warehouses operating either on premises, in a third party cloud or hosted in the MicroStrategy Cloud. MicroStrategy offers high performance hosted data warehouse services. MicroStrategy also supports access to heterogeneous data sources via its MultiSource Option capability, which is included with the MicroStrategy Cloud Platform.

If you choose to maintain your database on-premises, a typical implementation involves establishing a VPN connection between the MicroStrategy Cloud and your database or data warehouse (See the section on MicroStrategy Cloud Secure Connectivity MCSC). The performance of this architecture can vary based on a variety of factors, including the physical distance between the MicroStrategy Cloud data center and the customer data source, the latency of the data connection, the bandwidth of the connection, the amount of usage and its query intensiveness, the query-response latency of the customer data source, and other variables.

MicroStrategy Cloud leverages framework capabilities that enhance performance including Intelligent Cubes, caching, and pushdown analytics. These capabilities reduce the query traffic between the MicroStrategy Cloud and data sources.



MICROSTRATEGY CLOUD AND CUSTOMER RESPONSIBILITY

MicroStrategy provides management and basic database administration functions. The administration offerings include environment setup, configuration, monitoring, as well as additional services designed to maintain the high availability of the environment. MicroStrategy is responsible for managing the physical implementation of the data warehouse environment and restricts access to the server instances running the data warehouse. As part of the warehouse services, MicroStrategy manages patching the environments at the server and database level.

MicroStrategy customers are responsible for logical administration of the data warehouse including data modeling, creation of the data structures, and application development related tasks. Application performance tuning and optimizations are the responsibility of the customer. With customers responsible for designing and developing database objects, they are also responsible for change control and change management of database objects, and handling migrations between development, test, and production environments.

As customers are responsible for the data in the MicroStrategy Data Warehouse Services, they are responsible for implementing security best practices on the data warehouse. MicroStrategy personnel will have limited access to customer data with only critical administrators and support personnel specifically granted access by the customer. As a result, customers are responsible for all data they place in the MicroStrategy Cloud Data Warehouse service.

PERFORMANCE AND CONFIGURATION

The MicroStrategy Cloud operations managers have optimized the environment to enhance the performance of the configurations provided via the MicroStrategy Cloud Platform. The MicroStrategy Performance Lab runs extensive tests on the MicroStrategy Cloud environment providing optimization recommendations. These recommendations are used to tune the overall environment and establish the recommended default setting for new environments being set up in the cloud. Because each set of customer requirements and applications is different, MicroStrategy Cloud Engagement Managers meet with customers to review their requirements prior to implementation and configuration of an environment. Based on this analysis additional optimization settings may be applied.

As a premium service, we offer an optional initial performance assessment, which includes a series of tests that assess network performance between the MicroStrategy Cloud and your database. This assessment identifies specific optimizations to improve performance.

SERVICES

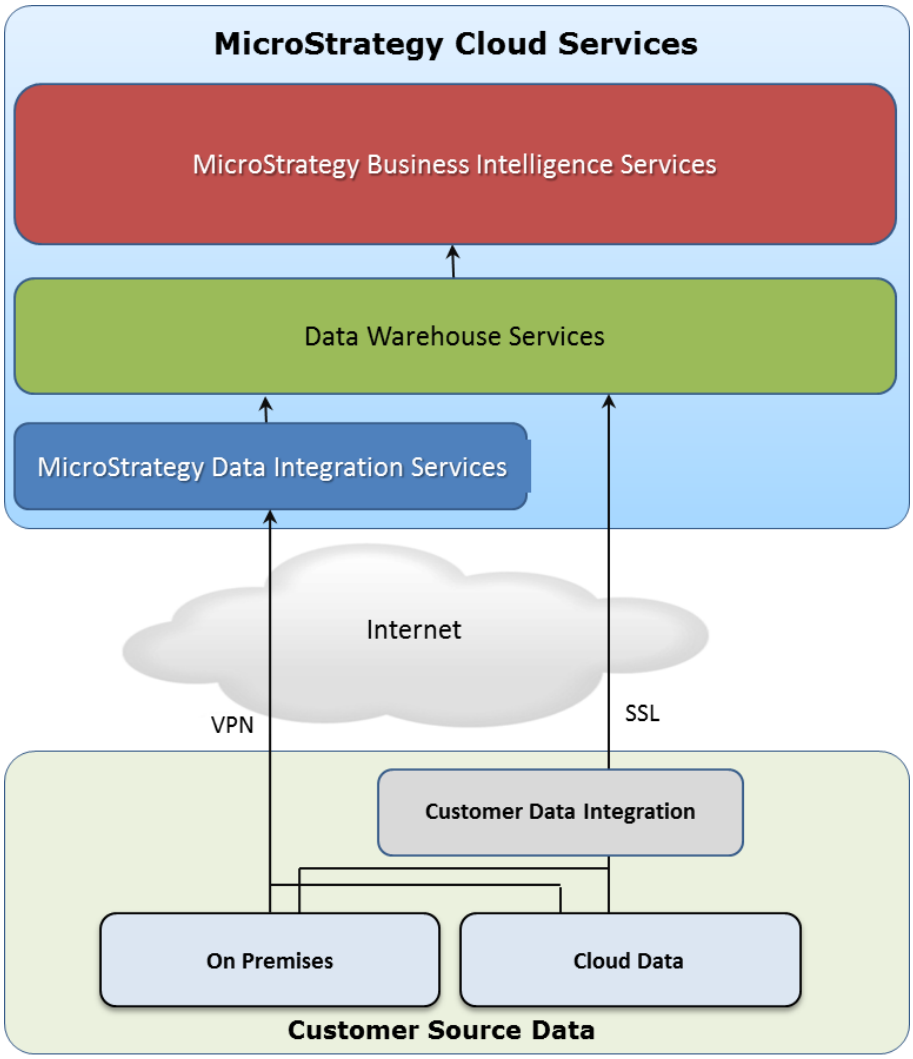
By default, customers are responsible for the design, development, change control and logical administration of the data warehouse, including data modeling, creation of data structures, and the tasks related to developing projects, reports, and documents. In addition, application performance tuning and optimizations are the responsibility of the customer. If desired, MicroStrategy Professional Services can be contracted to provide or assist with system tuning. Data loading, quality, and cleansing are responsibilities of the customer. MicroStrategy offers various Data Integration service options to load and validate data in the customer environment. Please contact your MicroStrategy Account Executive for more details.

DATA WAREHOUSE MANAGEMENT AND ACCESS

The environment is managed with a utility server provided as part of the MicroStrategy configuration infrastructure. The utility server's tools provide access to build and manage the customer's database instance. Access to the utility server is provided via Web VPN. Once environment configuration has been completed, details for connecting to the utility server are provided by MicroStrategy as part of your Connectivity Information sheet.

DATA MANAGEMENT AND LOADING

Data can be loaded into MicroStrategy Cloud Data Warehouse Services in multiple ways. MicroStrategy provides a full suite of Data Integration Tools to load your data. For more information, see *Data Integration Services*, above. If you already have internal data integration tools, they can be connected to MicroStrategy Cloud Data Warehouse Services to manage data in the warehouse environment. Please speak with your Cloud Engagement manager for full details.



MICROSTRATEGY CLOUD INFRASTRUCTURE AS A SERVICE

The MicroStrategy Cloud Infrastructure as a Service (IaaS) offering is an optional support service that provides customers with infrastructure resources to support their business intelligence environment. MicroStrategy Cloud can provide storage, network, and compute infrastructure. These resources require that the MicroStrategy Cloud Business Intelligence server be purchased in conjunction.

Storage: By default, the MicroStrategy Cloud Business Intelligence Service comes with a 35 Gig block of storage that is available for customers to use. Typically this storage is utilized for images, files, video, plug-in development and other files needed to support the MicroStrategy Business Intelligence environment. Often times this dedicated storage space does not provide adequate space for files needed for data integration, data warehouse, and business intelligence development. MicroStrategy Cloud provides the option to purchase additional storage. This storage is integrated into the customer environment and accessible via the customer FTP services, utility box, and other cloud systems.

Compute: MicroStrategy Cloud Services offer a wide array of tools to build out enterprise scale business intelligence applications. Even with the tools available, the MicroStrategy Platform cannot offer all of the applications and services that a company may require. To enable customers to implement their own software or third party software not supported by the MicroStrategy Cloud, a Compute IaaS offering is available. With the Compute IaaS offering, customers are able to select from a pre-defined list of virtualized compute instances sized (RAM, CPU, Disk Space) to meet their application needs. In addition, they have a choice between a specified list of Windows and Linux operating systems. With the Compute IaaS, customers are provided admin level access to the compute nodes. This enables the installation and development of applications that can be integrated into the Business Intelligence applications. In the Compute IaaS model, MicroStrategy will provide monitoring of the compute environment and provide operating system level patching. Customers are responsible for the maintenance and support of any software application they install on the Compute IaaS nodes as well as licensing for software they install in the MicroStrategy Cloud environment. It is the customers' responsibility to ensure the software is secure and properly patched and licensed. MicroStrategy can request at will review that the Compute IaaS system are in compliance. The MicroStrategy Compute IaaS offering is designed to support business intelligence applications and is not set to be a standalone service. MicroStrategy reserves the right to review applications and licensing of software running in the environment and if abuses are identified terminate customers' use of the service.

CLOUD PLATFORM SECURITY OVERVIEW

Security is a key concern. In a cloud environment, security responsibilities must be shared by the service provider and by the customer. Security topics covered in this document include:

For additional questions related to MicroStrategy Security practices in the cloud, send an email to Cloud@MicroStrategy.com.

SHARED SECURITY RESPONSIBILITY

MicroStrategy provides a secure infrastructure, controls, standards, and processes for our customers. The establishment of a customer instance in the MicroStrategy Cloud represents a partnership between MicroStrategy and the customer to provide a secure business intelligence environment.

In establishing the MicroStrategy Cloud environment, MicroStrategy assumes responsibility for the management and security of the network, hardware infrastructure, and software. When connecting to our service via the internet, our responsibility for the network includes the connections from the internet to our infrastructure. However, when utilizing VPN tunnels between the Customer and our Cloud Platform, the responsibility is shared. Our security practices include installing appropriate security patches, virus protections, upgraded hardware infrastructure, high availability, disaster recovery, and monitoring.

Our customers play a critical role in protecting their own environments. As part of the MicroStrategy Cloud environment, customers are provided access to build projects, reports, and documents, manage user access, define password policies, and perform various development, maintenance, and administrative tasks. Customers must take responsibility internally to protect the accounts that access their systems to prevent unauthorized access. MicroStrategy provides the ability to track and audit changes in the environment, but the customer must ensure that accounts are protected, password policies are followed, and application access is controlled.

Customers are also responsible for the management of user access. MicroStrategy will provide a set of tools that allow customers to add, modify, and delete user access. The tools permit management of users and groups. As part of user management, customers will provide password management policies which can be integrated into the MicroStrategy platform. MicroStrategy recommends that companies implement strong password policies.

Personally Identifiable Information and Customer Data Protection

You are solely responsible for the development, content, operation, maintenance, and use of Your Content. You are solely responsible for the compliance of your Content with the MicroStrategy's Cloud Platform Policies and all

laws that may apply to your data including those in your location as well as the data center location. You are responsible the handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Content violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act. You are responsible for properly configuring and using the Service Offerings and taking your own steps to maintain appropriate security, protection and backup of Your Content, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content. MicroStrategy Cloud Platform log-in credentials and private keys generated by the Services are for your internal use only and you may not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

CONFIGURATION MANAGEMENT

To validate network and infrastructure integrity, appropriate patch management protocols of integrated third-party products will be observed. MicroStrategy Cloud operations managers subscribe to automatic notifications for patches that are released by major vendors such as Microsoft, RedHat, Cisco, etc. In addition, MicroStrategy Cloud operations managers will check periodically for patches and releases that may be unannounced. MicroStrategy will assess whether a released patch is a service pack, feature upgrade, or security patch to establish the priority of deployment and appropriate procedure for release.

Each potentially applicable patch will be evaluated to determine whether it is applicable to the environment and how, when, and whether it should be deployed. Any patches proposed for implementation will be subject to appropriate isolated testing and verification prior to deployment. Enterprise systems will be patched after approval from MicroStrategy. The MicroStrategy Cloud Systems Engineering Team will follow standard procedures for migrating patches into production, including notifying field or remote users when a patch may be unknown to, but of importance to, a MicroStrategy customer.

The MicroStrategy Cloud team will notify end users and rely upon their compliance when a security patch should be installed to end user machines. Where possible, MicroStrategy will work with customers to minimize the impact of patches and maintenance and work around customers schedules. In some cases, due to system wide maintenance and after providing you reasonable notice, MicroStrategy will solely decide when maintenance will be applied to the Cloud customer environments. Patches will be managed by patch management software. The MicroStrategy Cloud team will use automated software deployment, whenever possible, to implement those patches designed to repair security vulnerabilities.

MICROSTRATEGY CONTROL ENVIRONMENT

MicroStrategy Cloud leverages and shares various aspects of MicroStrategy's overall control environment in the delivery of our Cloud services. The MicroStrategy Cloud controls are based on the Cloud Security Alliance control matrix. As such, MicroStrategy is able to map its controls to the most common industry control frameworks including COBIT, NIST, ISO27001/2, PCI, HIPAA, etc.

An industry-leading third party is responsible for the monitoring and Level 1 escalation within the MicroStrategy Cloud environment. This firm operates NOCs around the world and offers complete 24x7 environment and security monitoring services as well as a highly tested and accepted set of controls for monitoring and managing solutions such as ours.

MicroStrategy Cloud operates from a co-located data center. MicroStrategy personnel manage Level 2 and Level 3 escalations. Our hardware and software partners in the MicroStrategy Cloud initiative also provide Level 3 escalation coverage.

Change-management and patch-management audit trails are captured for changes implemented within the Cloud infrastructure and customer environments.

NETWORK SECURITY

MicroStrategy has architected the MicroStrategy Cloud Secure Connectivity (MCSC) infrastructure to establish secure connectivity between the MicroStrategy Cloud infrastructure, the customer's data center, and devices. The MCSC provides a secure connection between MicroStrategy and the customer's network for the MicroStrategy Cloud environment to access data from the customer environment. The MCSC is built on a secure computing infrastructure inside an isolated segment of the MicroStrategy Cloud network and is managed by MicroStrategy Information Systems professionals. The MCSC uses equipment that is self-contained and MCSC security practices are designed to protect electronic information and validate system integrity.

As part of a customer environment, each customer will be provided 3 connections between customer's data centers and the MicroStrategy Cloud environment as part of the initial service. Additional connections can be purchased by contacting your MicroStrategy Account Executive.

The MCSC is a virtual network environment. The physical MCSC is located in MicroStrategy's core data center and access is restricted to authorized personnel. Computing equipment in the MCSC is specifically and exclusively designated to be used by MicroStrategy Cloud customers. Access to configurations is limited to the authorized network professionals at MicroStrategy. Secure Shell (SSH) is used to access the network devices.

A secure firewall is used to protect and control network traffic. The firewall is configured to hide internal IP addresses using Static Network Address Translation (SNAT) and Static Port Translations (SPAT). External customer networks access the MCSC through a secured Virtual Private Network (VPN) tunnel. VPN connections can be configured to the specifications of external parties that are recognized by the security community standards, and alternative access methods can be granted based on customer requirements.

Virtual Local Area Networks (VLANs) are used to grant or deny access of specific MSCS machines to specific external networks. Each customer is designated an individual VLAN to provide a network separate from other customer networks. These networks cannot communicate with each other and users within the network cannot access one VLAN from another. Each customer environment can be configured for customer specifications. MicroStrategy Technical Support Engineers connect to the MCSC via Web VPN to work so that the engineer's machine does not directly access the customer's corporate network. This secure connectivity helps to prevent the spread of malicious traffic between networks.

By default MCSC computers do not have external access to the public Internet, unless specifically requested by the customer. Network monitoring and connection tracking systems are used in the MCSC and network connections are logged. Wireless computer network technology is not used inside MCSC.

IPSec VPN tunnels may also be configured to add layer of security for data transmissions between the MicroStrategy Cloud Platform and customer networks. Our network engineers work closely with your network team to establish either IKE Phase 1 (ISAKAMP) or Phase 2 (IPSec) tunnels per your requirements. During the configuration, we have your network team fill out the requirements and our network engineers apply these parameters to your Cloud environment.

MCSC SYSTEMS ENVIRONMENT

Restrictive permissions to files, services, and system settings are applied to MCSC computers. Access Control Lists (ACLs) are used to limit access. Unnecessary operating system services are removed or disabled before system deployment in MCSC. Users are required to authenticate using a unique username and password to access any MCSC computer. An up-to-date antivirus scanner is installed on MCSC computers and vulnerability scans are

conducted on MCSC computing equipment regularly. Security and other important patches provided by MCSC equipment vendors are routinely reviewed and applied by MicroStrategy Information Systems professionals. A Cloud support VLAN contains Windows Server Update Services (WSUS) and antivirus (AV) servers which provide appropriate updates to each network.

Virtual machines are deployed in the MCSC to support each customer configuration and they are governed by the same system security practices of physical machines.

US data centers supporting the Cloud Platform are SOC 1 Type II compliant and EMEA Data Centers supporting the Cloud Platform are ISO 27001 compliant. MicroStrategy reviews data center compliance on an annual basis to ensure that our providers continue to meet the standards.

SECURITY LOGGING

Inbound and outbound connections to the MCSC are logged. The data is encrypted, so that MicroStrategy cannot see data at the network layer. Only information such as connection source and destination IP and ports can be seen.

Firewall logs are mixed among the different customer environments. MicroStrategy requires five business days to fulfill any customer request for access to firewall logs for their environment. These requests will be performed on a time-and-materials basis to prepare logs specific to the customer's environment. It is not technically feasible to separate customer logs at the network level. Application logging is performed on a case-by-case basis.

Logs are retained for twelve months.

PHYSICAL SECURITY

The MicroStrategy Cloud Platform infrastructure is operated in co-located data centers. The data center provides an array of controls, monitoring tools, and physical intrusion detection systems to provide controlled access to systems.

The data centers are operated by a third party operator and designed to provide physical security of IT assets. The data centers are staffed 24 hours a day, 365 days a year. The data centers are built in low profile buildings with no signage and high grade security features. The centers are designed to prevent unauthorized access and track authorized access to the center.

The MicroStrategy data center partner uses a patented multi-level security tracking system using a five-layer approach to control physical access. Access to the data centers is by appointment only. Once inside, biometric hand-readers, sign-in procedures, and visual confirmation are required prior to granting access. The center uses hundreds of security cameras and hand geometry readers to continuously monitor critical areas of the data centers as well as customer cages.

Within the data center, the MicroStrategy Cloud infrastructure has been installed in an isolated environment, configured in its own set of cages, isolated from other customers and other MicroStrategy environments within the data center. The cages are physically secured and locked to prohibit unauthorized access. The MicroStrategy Security team keeps a list of MicroStrategy employees that have been granted access to the environment.

BACKUP POLICY

MicroStrategy Cloud backup policies and procedures are designed to reduce downtime to the customer should an unforeseen incident occur that impacts the quality or availability of the customer's data. These backup procedures are designed as part of an overall effort to provide high levels of availability to MicroStrategy Cloud customers.

The MicroStrategy Cloud team will back up the following customer components on a nightly basis:

- MicroStrategy environment including metadata
- Customer access control lists
- Virtual environment parameters and settings
- Applicable audit logs

Backup copies will be maintained in multiple secure sites to provide business continuity should a major incident occur. However, as these backups are point-in-time, MicroStrategy cannot guarantee that all data can be recovered. The MicroStrategy backups should not be construed as a substitute for customer backups of critical data.

Metadata backup copies will be maintained for a period of 30 days. The data warehouse backups will be kept for a period of two weeks. Backups can be restored on customer request, but will not exceed more than five such requests in a month. If customer requests exceed five, the customer will be billed at $150 an hour for the labor needed to fulfill the request.

MONITORING

MicroStrategy Cloud has implemented an integrated set of monitoring and management capabilities. These monitors are designed to proactively notify the MicroStrategy Cloud team of any issues that cause system failures or performance degradation within the environment. Agents are placed on the various tiers of the MicroStrategy Cloud framework to monitor hardware, storage, networking, virtualization, operating system, and applications, providing real-time visibility into the environment.

The environment is monitored 24x7 by the Global Network Operations Center (NOC). The NOC continuously monitors the environment analyzing overall stability and performance remain within appropriate thresholds. When the monitors alert that key thresholds are exceeded or systems are non-responsive, resources are notified.

If problems are identified, on-call resources are provided with scripts to help troubleshoot and identify the cause of problems and perform tasks to resume systems to normal performance. If the support and monitoring teams are unable to resolve the issues directly, a set of well-defined escalation procedures and on-call schedules are used to bring in the appropriate resources to resolve the problem.

For larger incidents impacting multiple areas of the framework or major incidents that cannot be resolved quickly, an incident response team is formed. The incident response team is assigned a lead responsible for managing the issues as well as a communication lead responsible for notifications and documentation of the issue. The team remains intact until the issue is closed. Upon closure of a major incident, the team debriefs to document the root cause of the issue to avoid recurrence of the problems.

MICROSTRATEGY RISK MANAGEMENT

MicroStrategy conducts an annual assessment of risk based on the strategic business plan and the strength of the controls needed to mitigate or reduce risk. As part of this assessment, business leaders are asked to identify the risks for their area of responsibility. In addition, the leaders will assess how likely it is that the risk will occur, and

the impact of the risk. The annual risk assessment allows MicroStrategy to focus their attention on the mitigation of the highest probability and largest impact risks.

MicroStrategy leverages internal risk management and internal audit functions to provide independent assessments of risk as part of an on-going cycle of audit. Third-party auditors are leveraged to provide a final assessment of the control framework for the company and validate that MicroStrategy is executing controls as documented.

MicroStrategy Cloud Security maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy. MicroStrategy performs weekly internal vulnerability scans of the MicroStrategy Cloud environment, as well as quarterly comprehensive external scans of the MicroStrategy Cloud environment and a yearly penetration test.

Customers may request to conduct their own scans of the MicroStrategy Cloud environment as long as these scans are focused only on the customer's instances and do not violate MicroStrategy Cloud's Acceptable Use Policy. The customer must request advanced approval for scans. A customer may request permission by emailing Cloud@microstrategy.com. Please provide at least 30 days prior notice for any scanning activity.

DATA RETENTION & DESTRUCTION POLICY

MicroStrategy has a commitment to protect the assets provided by customers and partners. One of the most critical assets is the data that is entrusted to MicroStrategy as part of the MicroStrategy Cloud Service. MicroStrategy is committed to the protection of this data while under contract with customers and its destruction when MicroStrategy and customers determine it is necessary to terminate the relationship.

DATA RETENTION

MicroStrategy has implemented a data and record retention policy designed such that documents are retained in a uniform format for a specified period of time based on a defined retention schedule. MicroStrategy employees, contractors, and its directors are responsible for following the policies outlined in the Data Record Retention Policy. Policies covered under this policy include:

1. Retains records as necessary for business purposes, including maintaining the continuity and availability of records in the event of a disaster or hardware failure.
2. Retains records in accordance with applicable federal and state laws.
3. Retains records relevant to pending or reasonably anticipated legal proceedings, consistent with the company's legal obligations.
4. Retains records as necessary for tax purposes.

The Data Record Retention Policy also specifies policies related to the destruction of documents that are no longer required for business, legal, tax, or other reasons. As part of the data destruction policy, the method for proper document destruction and disposal is defined.

Customer data created by MicroStrategy as part of conducting business falls under the MicroStrategy Data Record Retention Policy and will be managed as such.

CUSTOMER-PROVIDED DATA

Data that a customer provides to MicroStrategy includes, but is not limited to, business intelligence metadata values and descriptions, database schemas, ETL workflows and routines, data content (in database and text files), database backups, virtual machine images, user access information, and custom data manipulation code.

Data provided by the customer to MicroStrategy will be removed from the MicroStrategy environment and deleted within 30 days of termination of an agreement.

The customer may request, in writing, copies of the data to be provided. Such requests must be made prior to the termination of the agreement. Such copies will be subject to a fee based on the time required to fulfill the request.

MICROSTRATEGY CERTIFICATIONS AND ACCREDITATIONS

MicroStrategy's US data center locations are fully SOC 1 Type II compliant and leverage state-of-the-art biometric controls, stringent controlled entry processes, and video surveillance to provide security. The international data centers are ISO certified including ISO 27001:2005. Customers may request to review relevant SOC and/or ISO Reports for our data centers.

MICROSTRATEGY EMPLOYMENT PRACTICES

MicroStrategy is dedicated to creating and maintaining a work environment that develops and values employees, providing opportunities for them to contribute to the company's business success. MicroStrategy protects the personal welfare of employees with a work environment that does not tolerate unlawful discrimination, harassment, retaliation or violence, and requires adherence to the Federal Drug-Free Workplace Act and applicable environmental health and occupational safety laws and regulations.

EQUAL EMPLOYMENT OPPORTUNITY

MicroStrategy maintains policies for equal opportunity and advancement for qualified individuals without distinction or discrimination based on age, race, color, religion, creed, sex (including pregnancy, childbirth, or related medical conditions), marital or family status, national origin, ancestry, physical or mental disability, medical condition, veteran status, sexual orientation, or any other consideration prohibited under applicable law.

BACKGROUND SCREENING

MicroStrategy conducts pre-employment background screening on all applicants for employment. As permitted by law, MicroStrategy also conducts background screening on current employees who hold certain designated positions as circumstances warrant. Such background screening is done in accordance with applicable federal, state, and local laws.

ETHICAL STANDARDS

MicroStrategy is committed to upholding the integrity of the company through ethical business practices. Ethical conduct on the job is simply a matter of dealing fairly and honestly with MicroStrategy, fellow employees, customers, suppliers, competitors, investors, and the public. MicroStrategy employees are expected to avoid any action that results in or gives the appearance that they are using their employment at MicroStrategy for personal gain.

Every MicroStrategy employee is expected to adhere to the following company standards for activity in business-related locations or functions at all times:

- Treat customers and suppliers in a fair and honest manner
- Conduct the company's business with integrity
- Conduct the company's business within all applicable laws
- Maintain efficient, proper standards of work performance
- Maintain professional conduct during all company business and events
- Adhere to all work-related written and verbal company policies and instructions
- Maintain MicroStrategy business offices as clean and safe work environments

MicroStrategy employees are expected to always judge a proposed course of action based on ethical standards outlined in the MicroStrategy Employee Handbook.

EMPLOYEE CODE OF CONDUCT

All MicroStrategy employees are required to sign, indicating that they:

- Received a copy of, or have convenient access to, the Code of Conduct
- Read and understood the Code of Conduct
- Will act in accordance with the Code of Conduct to the extent permissible under applicable law
- Understand that the provisions contained in the Code of Conduct: (i) represent policies of MicroStrategy Incorporated and its subsidiaries and (ii) are applicable to all employees, officers and directors of MicroStrategy Incorporated and its subsidiaries
- Are obligated to bring to the attention of the appropriate personnel (as described in the Code of Conduct) any suspected violations of law or of the Code of Conduct
- Comply with, and will continue to comply with, the Code of Conduct

CONTRACTING

MicroStrategy performs background screening of contractors performing work on behalf of the company.

DATA BREACH POLICY

The MicroStrategy Cloud environment is developed to block any attempted hack of its systems or data. Port scanning or network scanning tools are strictly forbidden within the environment. MicroStrategy does not allow customers to install third-party monitoring or direct access to our core monitoring systems without agreement from the Cloud Operations team.

In the case that the MicroStrategy Cloud Team determines an anomalous event including, but not limited to, Denial of Service, Malicious Code, Unauthorized Access, Inappropriate Use, Physical Breach, and Data Breach, to be deemed a security incident; the team will immediately activate its Computer Security Incident Response Plan (CSIRT). The plan includes provisions for prompt response including Notification, Analysis, Containment, Eradication, Recovery as well as timely Reporting to appropriate parties.

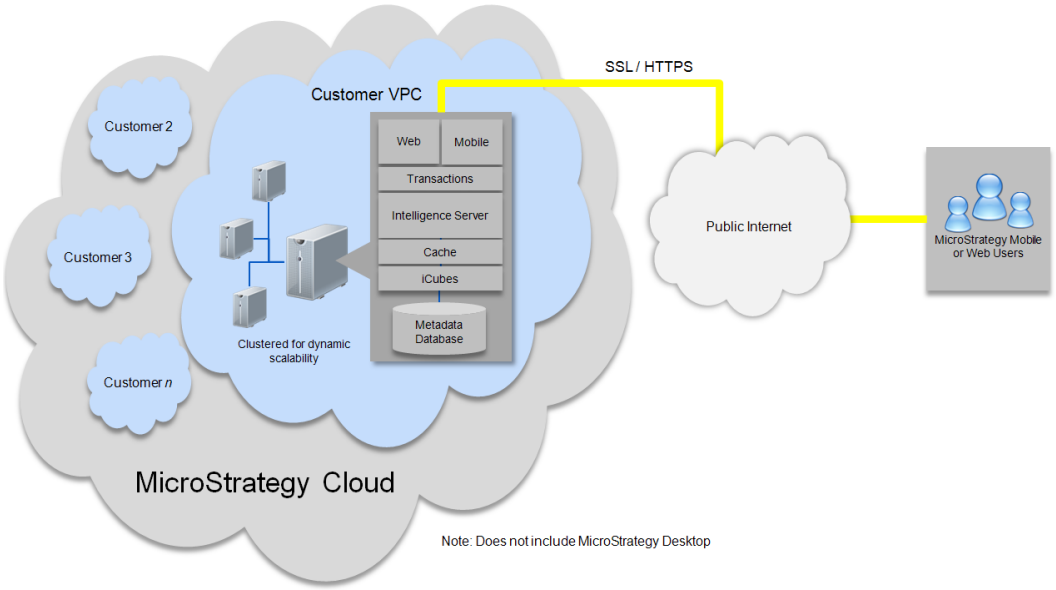
DOMAIN URL DEFINITION

Each MicroStrategy Cloud customer is given a separate URL to access the service. MicroStrategy provides a default domain for companies defined as `yourdomain.cloud.microstrategy.com`. You can request additional domains for your company at additional charge to cover the cost of security certificates required to support the domain. Contact a MicroStrategy Cloud expert for questions regarding custom domain mapping to a custom URL such as `cloudBI.yourdomain.com`.

ACCESSING THE MICROSTRATEGY CLOUD

Upon handoff of the MicroStrategy Cloud environment, designated customer representatives are provided a specification document outlining items related to their service. This document includes the configuration and connectivity details required to access their system.

MicroStrategy offers two options to access the Cloud Environment. The first method establishes a VPN connection between a customer network and the MicroStrategy Cloud. With this method, the MicroStrategy Cloud servers are not exposed directly to the Internet and appear as a set of machines on your private intranet. The second method allows the MicroStrategy Cloud servers direct access to the public Internet. This method is implemented upon customer request. By default web connectivity is set up using SSL/HTTPs.



The basic connection to MicroStrategy Cloud supports single factor authentication. Two-factor authentication is offered for an additional setup charge.

DEVELOPER ACCESS

Developers access MicroStrategy Cloud Platform using a Web VPN connection. Customer development teams are provided individual user accounts to access the development environment to build projects, reports, and

documents. MicroStrategy Architect is required to work on MicroStrategy Cloud systems. A monthly fee applies per user.

MICROSTRATEGY CLOUD PLATFORM SERVICE LEVEL AGREEMENT

During the term of you subscription, MicroStrategy shall use reasonable commercial efforts to ensure that the Online Service is available to you 99.9% of the time in any calendar month. In the event you experience additional Unavailability due to MicroStrategy's failure to provide the Online Services and provided you are running the latest approved version of the MicroStrategy Technology, you will be eligible to 1) receive Credits, as described below or 2) an extension of the license term for such licensed software equal to such credit.

To receive a service credit, the customer must submit a request to MicroStrategy within fifteen (15) days following the month in which the outage event(s) occurred. The service credits set forth in the table below are customer's sole and exclusive remedy when the uptime levels listed below fall below the stated levels. You understand and acknowledge that you may also engage in conduct that may cause your cloud based business intelligence environment to be unavailable and that MicroStrategy is not responsible for downtime experienced by a customer as a result of customer activity or neglect.

MicroStrategy's Service Level commitment covers equipment and software under MicroStrategy's direct control; including hardware (network, systems, storage) and software (database, ET&L, MicroStrategy, security) supported by the MicroStrategy Cloud framework.

This SLA does not cover downtimes as a result of issues related to applications built on the MicroStrategy platform including: project, report, and document design issues; migration problems related to customer design; ETL application design problems; Internet outages; improper database logical design and code issues; factors outside of our reasonable control; downtime related to scheduled maintenance; general internet unavailability and other application issues out of the reasonable control of MicroStrategy.

Uptime Table

Period	Monthly Uptime Percentage
Starting January 1st 2013	99.9%

Service Credit Table

Period	Uptime	Service Credit	
Starting January 1st 2013	99.9%	99.90% to 99.84%	1.00%
		99.83% to 99.74%	3.00%
		99.73% to 95.03%	5.00%
		95.02% or less	7.00%

"Applicable Monthly Service Fees" means the total fees actually paid by you for the Online Services that are applied to the month in which a Service Credit has accrued.

"Downtime" means the total minutes in a month during which you report that the Online Services are unavailable to you multiplied by the number of affected users, excluding unavailability of the Online Services due to limitations described above.

"Service Credit" is the percentage of the Applicable Monthly Service Fees credited to you following claim approval.

"Monthly Uptime Percentage" for the Online Services is calculated by the following formula:

(Total number of minutes in a month – Downtime)./ Total number of minutes in a month * 100.

Note: The above terms shall be adjusted and used in support of new Data Centers as they are brought online around the world.

Note: Services credits are listed as hours.

If we fail to meet the minimum Monthly Uptime Percentage described above for the Online Services, you may submit a claim for a Service Credit.

You must submit a claim to technical support at MicroStrategy that includes: (i) a detailed description of the event that resulted in Downtime; (ii) information regarding the duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the incident at the time of occurrence.

We must receive the claim and all required information by the 15th day of the calendar month following the month in which the Incident occurred. For example, if the Incident occurred on February 10, we must receive the claim and all required information by March 15. We will then evaluate all information reasonably available to us and make a good faith judgment on whether a Service Credit is owed. You may not unilaterally offset any invoice for claimed Service Credits.

If you purchased the Online Service from a reseller, you will receive a service credit directly from your reseller and the reseller will receive a Service Credit directly from us.

MICROSTRATEGY UPGRADE POLICY AND PROCESS

As new versions of the underlying MicroStrategy business intelligence platform are released, MicroStrategy Cloud Platform is updated with the enhancements contained in those releases. For customers subscribing to the Cloud with a clustered environment, the update process proceeds in the following ways depending on the type of platform update. For customers subscribing to a single-node environment, the cloud team will upgrade the single-node at the customer's request. Recovery of single node upgrades is performed via a rebuild of the system and a restoration of a backup of the previous version metadata.

A. Minor patches and upgrades

    1. MicroStrategy maintains a scheduled two hour maintenance window on Wednesday and Saturday night of each week.

    2. MicroStrategy posts notification of plans to deploy patches, providing customers an opportunity to raise concerns regarding the application of patches.

    3. If no concerns are raised about a patch, MicroStrategy applies patches during the window of scheduled downtime. Scheduled maintenance downtimes do not count against MicroStrategy's uptime SLA.

B. Major releases

    1. MicroStrategy performs rigorous testing of major release versions prior to upgrading customer environments to maintain stability.

    2. MicroStrategy provides a timeframe within which customers are able to schedule a time, allowing customers to minimize the impact of the transition.

3. For customers subscribing to MicroStrategy environments with clustering services, MicroStrategy creates an instance of your system based on the upgraded software platform to maintain your service during the upgrade. This instance runs in parallel with your production environment for a period of two weeks, during which time you may test the system using MicroStrategy Integrity Manager or other means. MicroStrategy also conducts its own tests during this time period.

4. At the end of the two week period, users of the old system are redirected to the new instance, and the old instance becomes unavailable.

All costs associated with these processes are included in your MicroStrategy Cloud Platform contract. MicroStrategy can accommodate additional, non-standard services or a customized upgrade process, for example, to accommodate more extensive user acceptance testing, subject to additional fees. New functionality is available to customers as soon as an upgrade has been completed. To the extent that the use of any new functionality is dependent on business intelligence solution design, the customer maintains control over the new functionality in its projects, reports, and documents.

MAINTENANCE PLANNING

MicroStrategy Cloud uses maintenance windows in support of planned maintenance activities. If the customer wishes to reschedule planned maintenance, the customer must submit a request to do so. Our maintenance windows may be scheduled from 2:00 AM – 5:00 AM on any Wednesday or Saturday during the year. Times are relative to the location of the primary Data Center, which hosts the customer's Cloud environments. We will provide our customers at least 48 hours advanced notice when maintenance window is activated. During these scheduled interruptions, MicroStrategy Cloud systems may be unable to transmit and receive data through the provided services. Customer systems should include a process to pause and restart the applications around planned maintenance activities.

When it is necessary to execute emergency maintenance procedures, MicroStrategy notifies the customer by email and addresses pertinent concerns in an expedited manner.

CLOUD PLATFORM SUPPORT

MicroStrategy Technical Support provides MicroStrategy Cloud Platform users with support 24 hours a day, 365 days a year. Many of the features from MicroStrategy support are available to MicroStrategy Cloud customers including:

- Access to the MicroStrategy Knowledge Base for technical and troubleshooting documentation
- Access to the MicroStrategy Discussion Forums, in which customers participate in open discussions and share best practices
- Access to on-line case logging through the MicroStrategy support site

BUSINESS AND SUPPORT OPERATIONS

MicroStrategy is headquartered in Tysons Corner, Virginia with the Cloud Services run out of multiple geographically dispersed locations including:

- Ashburn, VA – Data Center
- Seattle, WA – Data Center (Beginning Q2, 2013)
- Slough, England – Data Center
- Tysons Corner, VA – Operational Support
- Chiswick, England – Operational Support
- Warsaw, Poland – Operational Support
- Hangzhou, China – Operational Support

SUPPORT LIAISONS

Support liaisons are individuals designated by the customer in their license or maintenance agreement as a point-of-contact with MicroStrategy's support personnel. Technical Support services may only be obtained by support liaisons. The support liaisons maintain ownership of issues escalated into MicroStrategy Technical Support and as such, case-related communication is conducted with these named individuals. Your support agreement with MicroStrategy provides for a set number of support liaisons that are authorized to contact MicroStrategy Technical Support. Additional support liaisons can be acquired through the customer's account management team if needed. Customers may request to change their support liaisons six times per year. It is the customer's responsibility to advise MicroStrategy Technical Support if there are any existing support cases that should be transferred when a support liaison is changed.

CONTACT SUPPORT

Problems or questions related to MicroStrategy Cloud Platform must be reported to MicroStrategy Technical Support using the standard communication channels.

To contact MicroStrategy Technical Support access the MicroStrategy Global Support website: https://resource.microstrategy.com/support/

For priority-level 1 and 2 emergencies, the MicroStrategy Cloud 24x7 emergency number is: 1-855-CB1-MSTR (1-855-221-6787).

NOTE: 24x7 support is provided in English only.

MicroStrategy Cloud support follows the same processes as described in the MicroStrategy Technical Support Policies and Procedures - http://www.microstrategy.com/Support/Policies/.

LOGGING A CLOUD TECHNICAL SUPPORT CASE

To log a MicroStrategy Cloud technical support case, the designated support liaisons may contact MicroStrategy Technical Support via email, telephone, or by using the Online Case Tracking Interface, located on the MicroStrategy Support Site: https://resource.microstrategy.com/support. Only the designated support liaisons can log cases with MicroStrategy Technical Support. Upon logging a case, the support liaison receives a case identification that should be used for communications regarding this case.

When logging a case, be prepared to provide the following information:

- Personal Information
- Name
- Company and customer site (if different from own company)
- Contact information (phone and fax numbers, e-mail address)
- Case Details
- Configuration information, including MicroStrategy software product(s), version(s), and DSI in which the products are installed
- Full description of the case containing symptoms, error message(s), steps taken to troubleshoot the case thus far
- Log files or other supporting data
- Customer system impact

TYPES OF CLOUD PLATFORM CASES

MicroStrategy Cloud technical support cases are segmented in two different categories:

a) MicroStrategy product issues: issues are standard Technical Support cases and follow the priority and response guidelines outlined in section 3.3 of the MicroStrategy Technical Support Policies and Procedures document.
b) Cloud infrastructure issues: issues are referred to the MicroStrategy Cloud operations managers by Technical Support and follow the priority and response guidelines outlined below.

PRIORITIES AND RESPONSE GUIDELINES

Priority Level	Escalation Level	Definition	Priority Level Examples	Initial Response Time	Status Update
1	Critical (Immediate Action)	Critical component(s) are degraded or offline and the production systems are impacted.	Virtual application is unavailable.	< 2 Hours	Daily / As status changes
2	Major Within 8 Hours (Same Business Day)	Non-critical component(s) are degraded or offline and the production systems are impacted.	Reports are not delivered by Distribution Services	< 2 Hours	Daily / As status changes
3	Medium Within 48 Hours (2 Business Days)	Component(s) are degraded or offline but the production systems are NOT impacted. (e.g. Development, Test & Support Systems)	I-Cubes are not automatically refreshed in the development system.	< 4 Hours	As status changes
4	Low (As Time & Priorities Permit)	Little or no business impact.	How frequently snapshots of the VAPPs are taken?	< 6 Hours	As status changes

PROVIDING DATA TO MICROSTRATEGY TECHNICAL SUPPORT

During the course of troubleshooting and researching issues, it may be necessary to provide MicroStrategy Technical Support personnel with data from your systems (diagnostics, metadata copies, etc.). For the convenience of our customers, MicroStrategy provides several methods to transmit this data including, but not limited to, email, the MicroStrategy support site and the MicroStrategy download site. However, if the customer is sharing any confidential data which may be subject to government regulation, it is the customer's responsibility to transmit that data to MicroStrategy using MicroStrategy's secure FTP server. Customers should work with the Technical Support Engineer assigned to their case to coordinate any such data transfers. If MicroStrategy Technical Support requires information that might be stored on the cloud infrastructure, explicit approval from the customer is required for Technical Support to obtain this information from the MicroStrategy Cloud operations managers.